

PATENT ABSTRACTS OF JAPAN

(B)

(11)Publication number : 05-298174

(43)Date of publication of application : 12.11.1993

(51)Int.Cl.

G06F 12/00

G06F 12/00

G06F 13/00

(21)Application number : 04-101355

(71)Applicant : TOSHIBA CORP

(22)Date of filing : 21.04.1992

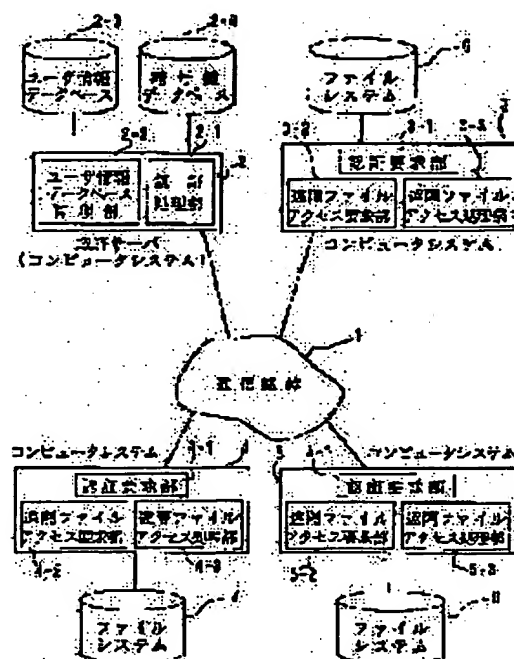
(72)Inventor : NUKUI HARUMI

(54) REMOTE FILE ACCESS SYSTEM

(57)Abstract:

PURPOSE: To improve the justification and safety of a file access.

CONSTITUTION: A remote file access request part 3-2 of a computer system 3 to be a remote file access request origin ciphers the authenticated certificate and the access request list acquired by the authentication server (computer system) 2 by a self-decoding key, prepares an access request packet by adding user identification information to the ciphered information, further ciphers it by the ciphering key of an access request destination computer system, and performs the access request of a remote file. A remote file access processing part 4-3 of a computer system 4 to be a remote file access request destination decodes the ciphered access request packet by the self-decoding key, acquires the ciphering key of a user from the authentication server 2 based on the user identification information obtained by further decoding, decodes the authenticated certificate and the access request list and performs the authentication of the user and the processing for the acceptance and rejection of the remote file access.



LEGAL STATUS

[Date of request for examination]

[Date of sending the examiner's decision of rejection]

[Kind of final disposal of application other than the examiner's decision of rejection or application converted registration]

[Date of final disposal for application]

[Patent number]

[Date of registration]

[Number of appeal against examiner's decision of rejection]

[Date of requesting appeal against examiner's decision of rejection]

[Date of extinction of right]

(19) 日本国特許庁 (J P)

(12) 公開特許公報 (A)

(11) 特許出願公開番号

特開平 5 - 2 9 8 1 7 4

(43) 公開日 平成 5 年 (1993) 11 月 12 日

(51) Int. Cl.

G06F 12/00

13/00

識別記号

545

537

351

庁内整理番号

F 8526-5B

H 8526-5B

E 7368-5B

F 1

技術表示箇所

審査請求 未請求 請求項の数 1 (全 6 頁)

(21) 出願番号 特願平 4 - 1 0 1 3 5 5

(22) 出願日 平成 4 年 (1992) 4 月 21 日

(71) 出願人 0 0 0 0 0 3 0 7 8

株式会社東芝

神奈川県川崎市幸区堀川町 7 2 番地

(72) 発明者 貫井 春美

神奈川県川崎市幸区柳町 7 0 株式会社東

芝柳町工場内

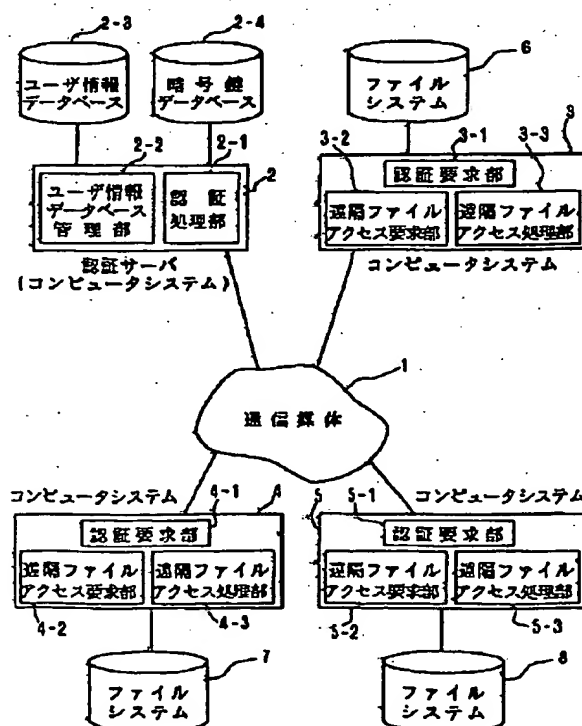
(74) 代理人 弁理士 木村 高久

(54) 【発明の名称】 遠隔ファイルアクセスシステム

(57) 【要約】

【目的】 ファイルアクセスの正当性と安全性を向上する。

【構成】 遠隔ファイルアクセス要求元のコンピュータシステム 3 の遠隔ファイルアクセス要求部 3-2 は、認証サーバ 2 から取得した認証済証明書とアクセス要求リストを自己の復号鍵で暗号化し、該暗号化された情報にユーザ識別情報を付加してアクセス要求パケットを作成し、さらにアクセス要求先コンピュータシステムの暗号鍵で暗号化し、遠隔ファイルのアクセス要求を行い、遠隔ファイルアクセス要求先のコンピュータシステム 4 の遠隔ファイルアクセス処理部 4-3 は、暗号化されたアクセス要求パケットを自己の復号鍵で復号化し、さらに復号して得られたユーザ識別情報をもとに認証サーバ 2 からユーザの暗号鍵を取得し、認証済証明書およびアクセス要求リストを復号し、ユーザの認証および遠隔ファイルアクセス許可の処理を行う。



【特許請求の範囲】

【請求項 1】複数のコンピュータシステムが任意の通信媒体を介して接続されたネットワーク上で、特定のコンピュータシステムが利用者情報を一括管理して発行する認証済証明書に基づいて、前記複数のコンピュータシステムに接続される遠隔ファイルシステムのファイルアクセスを行う遠隔ファイルアクセスシステムにおいて、遠隔ファイルアクセス要求元のコンピュータシステムは、前記認証済証明書とファイルアクセス要求リストを利用者固有の利用者識別情報をもとに暗号化し、該暗号化された情報と利用者識別情報をさらに前記特定のコンピュータシステムから取得したアクセス要求先コンピュータシステムの情報をもとに暗号化し、該暗号化された情報により前記遠隔ファイルのアクセス要求を行う遠隔ファイルアクセス要求手段を有し、

遠隔ファイルアクセス要求先のコンピュータシステムは、前記遠隔ファイルのアクセス要求を自コンピュータシステムがもつ情報により復号して利用者識別情報を得て、さらに該利用者識別情報をもとに暗号化されている前記認証済証明書とファイルアクセス要求リストを復号して利用者の認証および遠隔ファイルアクセス許可の処理を行う遠隔ファイルアクセス処理手段を有して、相互に認証を行うことを特徴とする遠隔ファイルアクセスシステム。

【発明の詳細な説明】

【0001】

【産業上の利用分野】本発明は、任意の通信媒体を介して接続された複数のコンピュータシステムから構成されるネットワークシステム上の遠隔ファイルシステムをアクセスする遠隔ファイルアクセスシステムに関する。

【0002】

【従来の技術】従来、複数のコンピュータシステムが任意に通信媒体を介して接続された分散環境においては、特定のコンピュータである認証サーバにより利用開始手続が行われ、正しいユーザと判断された時に、認証済証明書が発行され、さらに、その後この認証済証明書を再度認証サーバに提出し、サービス利用のための証明書を得ることによって利用可能になるという手続が行われていた。

【0003】これに対し、遠隔ノードのコンピュータシステムに存在する遠隔ファイルシステムをアクセスすることができる遠隔ファイルアクセスシステムにおいては、利用者識別子とファイル保護情報の組合せにより、遠隔ファイルアクセスの可否を判断するという単一ノード内と同様な一方的ファイルアクセス形態をとっていた。

【0004】このため、遠隔ノードのコンピュータシステムからファイルアクセスを要求した利用者が、本来の利用者識別子を所有する利用者であるという保証はなく、不正にアクセスされる可能性があるという問題点が

あった。

【0005】

【発明が解決しようとする課題】前述したように、複数のコンピュータシステムが任意の通信媒体を介して接続されたネットワーク上で、特定のコンピュータシステムが利用者情報を一括管理して発行する認証済証明書に基づいて、前記コンピュータシステムに接続される遠隔ファイルシステムのファイルアクセスを行う遠隔ファイルアクセスシステムにおいて、前記認証済証明書による要求元から要求先への一方向の認証であったため、遠隔のコンピュータシステムからファイルアクセスを要求した利用者が、本来の利用者識別子を所有する利用者であるという保証はなく、不正にアクセスされる可能性があるという問題点があった。

【0006】そこで、本発明は、かかる問題点を除去し、ファイルアクセスの正当性と安全性を向しした遠隔ファイルアクセスシステムを提供することを目的とする。

【0007】

【課題を解決するための手段】本発明は、複数のコンピュータシステムが任意の通信媒体を介して接続されたネットワーク上で、特定のコンピュータシステムが利用者情報を一括管理して発行する認証済証明書に基づいて、前記複数のコンピュータシステムに接続される遠隔ファイルシステムのファイルアクセスを行う遠隔ファイルアクセスシステムにおいて、遠隔ファイルアクセス要求元のコンピュータシステムは、前記認証済証明書とファイルアクセス要求リストを利用者固有の利用者識別情報をもとに暗号化し、該暗号化された情報と利用者識別情報をさらに前記特定のコンピュータシステムから取得したアクセス要求先コンピュータシステムの情報をもとに暗号化し、該暗号化された情報により前記遠隔ファイルのアクセス要求を行う遠隔ファイルアクセス要求手段を有し、遠隔ファイルアクセス要求先のコンピュータシステムは、前記遠隔ファイルのアクセス要求を自コンピュータシステムがもつ情報により復号して利用者識別情報を得て、さらに該利用者識別情報をもとに暗号化されている前記認証済証明書とファイルアクセス要求リストを復号して利用者の認証および遠隔ファイルアクセス許可の処理を行う遠隔ファイルアクセス処理手段を有して、相互に認証を行うことを特徴とする遠隔ファイルアクセスシステム。

【0008】

【作用】本発明は、複数のコンピュータシステムが任意の通信媒体を介して接続されたネットワーク上で、特定のコンピュータシステムが利用者情報を一括管理して発行する認証済証明書に基づいて、前記複数のコンピュータシステムに接続される遠隔ファイルシステムのファイルアクセスを行う遠隔ファイルアクセスシステムにおいて、遠隔ファイルアクセス要求手段は、遠隔ファイルア

クセス要求元のコンピュータシステムは、前記認証済証明書とファイルアクセス要求リストを利用者固有の利用者識別情報をもとに暗号化し、該暗号化された情報と利用者識別情報をさらに前記特定のコンピュータシステムから取得したアクセス要求先コンピュータシステムの情報をもとに暗号化し、該暗号化された情報により前記遠隔ファイルのアクセス要求を行い、遠隔ファイルアクセス処理手段は、遠隔ファイルアクセス要求先のコンピュータシステムは、前記遠隔ファイルのアクセス要求を自コンピュータシステムがもつ情報により復号して利用者識別情報を得て、さらに該利用者識別情報をもとに暗号化されている前記認証済証明書とファイルアクセス要求リストを復号して利用者の認証および遠隔ファイルアクセス可否の処理を行い、相互に認証を行う。

【 0 0 0 9 】

【実施例】以下、図面を参照して本発明の実施例について説明する。

【 0 0 1 0 】図 1 は、本発明の一実施例である遠隔ファイルアクセスシステムの構成ブロック図である。図 1 において、複数のコンピュータシステム 2 ～ 5 は通信媒体 1 に接続されている。コンピュータシステム 2 は、認証サーバであり、ネットワーク上のユーザ情報を一括管理するユーザ情報データベース管理部 2 - 2 とユーザのサービス利用可否を判断するための認証済証明書を発行する認証処理部 2 - 1 から構成されており、ユーザ情報およびユーザがネットワーク上で利用可能なサービス情報を管理するユーザ情報データベース 2 - 3 および暗号鍵データベース 2 - 4 が接続されている。コンピュータシステム 3 ～ 5 は、ユーザが一般に利用するコンピュータシステムであり、ユーザ名およびパスワードのユーザ情報を入力する認証要求部 3 - 1 ～ 5 - 1 と、他のコンピュータシステムへサービスを要求する遠隔ファイルアクセス要求部 3 - 2 ～ 5 - 2 と、他のコンピュータシステムからのサービス要求を受け付ける遠隔ファイルアクセス処理部 3 - 3 ～ 5 - 3 から構成される。なお、遠隔ファイルアクセス処理部 3 - 3 ～ 5 - 3 は、ファイルシステム 6 ～ 8 のアクセス許可リストを有している。

【 0 0 1 1 】図 2 は、遠隔ファイルアクセスの概要フローチャートである。図 2 において、まず、コンピュータシステム 3 ～ 5 の認証要求部 3 - 1 ～ 5 - 1 は、ユーザが入力したユーザ名・パスワードをもとに、認証サーバ 2 の認証処理部 2 - 1 にユーザの身元確認を要求し、正しいと判断されて認証済証明書が発行されることにより、ユーザの利用開始手続が完了する（ステップ 1）。次に、この認証済証明書は、コンピュータシステム 3 ～ 5 に保存される。コンピュータシステム 3 ～ 5 の遠隔ファイルアクセス要求部 3 - 2 ～ 5 - 2 は、認証済証明書をもとに遠隔ファイルアクセスの要求を行う（ステップ 2）。これに対し、コンピュータシステム 3 ～ 5 の遠隔ファイルアクセス処理部 3 - 3 ～ 5 - 3 は、遠

隔ファイルアクセス要求のファイルアクセス可否のチェックを行い（ステップ 2 3）、アクセス許可である場合には、認証済証明書を確証してファイルアクセスが行われる。

【 0 0 1 2 】図 3 は、認証済証明書のフォーマット図である。図 3 において、認証済証明書は、認証サーバのホスト名および認証サーバの位置を示すアドレスが格納されている。その他、ユーザ名、ユーザの識別を示すユーザ ID 番号、認証済証明書の発行時刻および有効期限が格納される。この認証済証明書をもとに、コンピュータシステムの遠隔ファイルアクセス要求部は、遠隔ファイルアクセスを行うことになる。

次に、認証済証明書を発行されたコンピュータシステム 3 のユーザがコンピュータシステム 4 のファイルアクセスを要求する場合を説明する。この遠隔ファイルアクセス要求は、コンピュータシステム 3 の遠隔ファイルアクセス要求部 3 - 2 が、アクセス要求バケットを組み立てて、該当ノードであるコンピュータシステム 4 の遠隔ファイルアクセス処理部 4 - 3 に転送することによって行われる。

【 0 0 1 3 】図 4 は、アクセス要求バケットの構成を示す図である。図 4 において、斜線部 4 1 の認証済証明書とアクセス要求リストは、コンピュータシステム 3 の要求ユーザの復号鍵で暗号化され、斜線部 4 0 のように、アクセス要求バケット全体は、遠隔ノードであるコンピュータシステム 4 の暗号鍵で暗号化されている。なお、アクセス要求リストは、対象ファイル名とアクセスの種類が含まれている。

【 0 0 1 4 】図 5 は、遠隔ファイルアクセス要求部の動作フローチャートである。図 5 において、まず、認証済証明書を認証サーバ 2 から受け取ると、コンピュータシステム 3 の遠隔ファイルアクセス要求部 3 - 2 は、遠隔ノードのコンピュータシステム 4 の遠隔ファイルのアクセス要求リストを作成する（ステップ 5 1）。次に、ファイルアクセスする遠隔ノードの暗号鍵を取得する（ステップ 5 2）。さらに、受け取った認証済証明書と作成したアクセス要求リストを、ユーザの身元保証を行うため、ユーザのみが知る復号鍵で暗号化する（ステップ 5 3）。さらに、ユーザ名、ユーザ ID、ステップ 5 3 で暗号化した情報からアクセス要求バケットを作成する

（ステップ 5 4）。その後、遠隔ノードの暗号鍵で暗号化する（ステップ 5 5）。ここで、この暗号鍵は、認証サーバ 2 の暗号鍵データベース 2 - 4 から取得する。その後、遠隔ノードの遠隔ファイルアクセス処理部に送信する（ステップ 5 6）。

【 0 0 1 5 】図 6 は、遠隔ファイルアクセス処理部の動作フローチャートである。図 6 において、まず、コンピュータシステム 4 の遠隔ファイルアクセス処理部 4 - 3 は、受信したアクセス要求バケットを自己のみが知る復号鍵で復号する（ステップ 6 1）。次に、アクセス要求

5

バケットが復号できたか否かを判定し(ステップ62)、復号できない場合は、ステップ69へ移行し、他のノードへの要求またはネットワーク上第三者によってデータが介在されたと判断して、遠隔ファイルアクセスの処理を否定し、中止する(ステップ69)。一方、復号できた場合は、アクセス要求バケットの中から、アクセス要求元のユーザ名を取り出し、このユーザ名により認証サーバ2の暗号鍵データベース2-4からユーザの暗号鍵を取得する(ステップ63)。さらに、この取得された暗号鍵により、アクセス要求リストを復号化する(ステップ64)。次に、アクセス要求リストが復号できたか否かを判定する(ステップ65)。復号できない場合は、アクセス要求リストがアクセス要求者のみが知るアクセス要求者の復号鍵で暗号化されているので、異なるユーザからのアクセス要求であるか、第三者により介在されたとしてアクセス要求を否定し、遠隔ファイルアクセス処理を中止する(ステップ69)。一方、アクセス要求リストが復号された場合は、アクセス要求リストの中から認証済証明書を取り出し、認証済証明書に含まれる認証済証明書の発行時刻と有効期限により、認証済証明書の正当性を判定する(ステップ66)。認証済証明書の正当性が確認されない場合は、ステップ55と同様に、遠隔ファイルアクセス処理を否定し、処理を中止する(ステップ69)。一方、認証済証明書が正当で

$$\text{発行時刻 } T_t \leq \text{現在時刻 } T_c \leq \text{発行時刻 } T_t + \text{有効期限 } T_l$$

(1)

次に、式(1)が成立する場合は、正当な認証済証明書として処理し(ステップ75)、式(2)が成立しない場合は、不正な認証済証明書として処理する(ステップ76)。

【0018】なお、以上の実施例においては、公開鍵暗号方式による遠隔ファイルアクセスシステムの例を示しているが、公開鍵暗号方式に限定するのではなく、システムとして最も適する暗号方式を採用すればよい。

【0019】このようにして、遠隔ファイルアクセスのファイルアクセス権のチェックは、認証証明書を用いて、アクセス要求者が、本来使用すべきユーザIDによりアクセス要求を行っているかの判断が可能となり、これによる身元保証を行った上で、ユーザIDとファイルアクセスリストによるアクセスチェックを行うため、正確にチェックすることが可能となり、ネットワーク上での遠隔ファイルアクセスシステムの正確性・安全性を向上させることが可能となる。

【0020】

【発明の効果】以上説明したように、本発明は、複数のコンピュータシステムが任意の通信媒体を介して接続されたネットワーク上で、特定のコンピュータシステムが利用者情報を一括管理して発行する認証済証明書に基づいて、前記複数のコンピュータシステムに接続される遠隔ファイルシステムのファイルアクセスを行う遠隔ファイルアクセスシステムにおいて、遠隔ファイルアクセス

6

あると確認できた場合は、さらに、アクセス要求をユーザ識別子(ユーザID)と遠隔ファイルアクセス処理部4-3が有するアクセス許可リストにより、ファイルアクセスの許可を判断する(ステップ67)。アクセス許可リストにユーザIDでのアクセス許可が登録されていない場合には、ステップ66と同様に、ファイルアクセスが否定され、アクセス処理が中止される(ステップ69)。一方、アクセス許可が登録されている場合に、初めて、ファイルアクセスが許可される(ステップ68)。

【0016】ここで、ステップ66における認証済証明書の正当性判断について、詳細に説明する。図7は、認証済証明書の正当性判断フローチャートである。図7において、まず、認証済証明書の中からユーザ名、ユーザIDを取り出し(ステップ71)、ファイルアクセス要求バケットのユーザ名、ユーザIDと等しいか否かを判断する(ステップ72)。ここで、等しくない場合は、不正な認証済証明書として処理される(ステップ76)。一方、ユーザ名、ユーザIDが等しい場合は、現在時刻 T_c 、発行時刻 T_t 、有効期限 T_l を取り出す(ステップ73)。次に、式(1)が成立するか否かを判断する(ステップ74)。

【0017】

要求手段は、遠隔ファイルアクセス要求元のコンピュータシステムは、前記認証済証明書とファイルアクセス要求リストを利用者固有の利用者識別情報をもとに暗号化し、該暗号化された情報と利用者識別情報をさらに前記特定のコンピュータシステムから取得したアクセス要求先コンピュータシステムの情報をもとに暗号化し、該暗号化された情報により前記遠隔ファイルのアクセス要求を行い、遠隔ファイルアクセス処理手段は、遠隔ファイルアクセス要求先のコンピュータシステムは、前記遠隔ファイルのアクセス要求を自コンピュータシステムがもつ情報により復号して利用者識別情報を得て、さらに該利用者識別情報をもとに暗号化されている前記認証済証明書とファイルアクセス要求リストを復号して利用者の認証および遠隔ファイルアクセス許可の処理を行い、相互に認証を行う。すなわち、従来の一方向的なユーザIDとアクセス許可リストの組合せによる遠隔ファイルアクセス権のチェックに加えて、アクセス要求者が本来利用するユーザIDによって要求しているかを認証することにより、アクセス要求者の身元保証を相互に行うようにしているため、遠隔ファイルシステムのファイルアクセスの正当性・安全性を向上することができるという利点を有する。

【図面の簡単な説明】

【図1】本発明の一実施例である遠隔ファイルアクセスシステムの構成ブロック図。

【図 2】 遠隔ファイルアクセスの概要フローチャート。

【図 3】 認証済証明書フォーマット図。

【図 4】 アクセス要求パケットの構成を示す図。

【図 5】 遠隔ファイルアクセス要求部の動作フローチャート。

【図 6】 遠隔ファイルアクセス処理部の動作フローチャート。

【図 7】 認証済証明書の正当性判断フローチャート。

【符号の説明】

1 通信媒体

2 認証サーバ

2-1 認証処理部

2-2 ユーザ情報データベース管理部

2-3 ユーザ情報データベース

2-4 暗号鍵データベース

3~5 コンピュータシステム

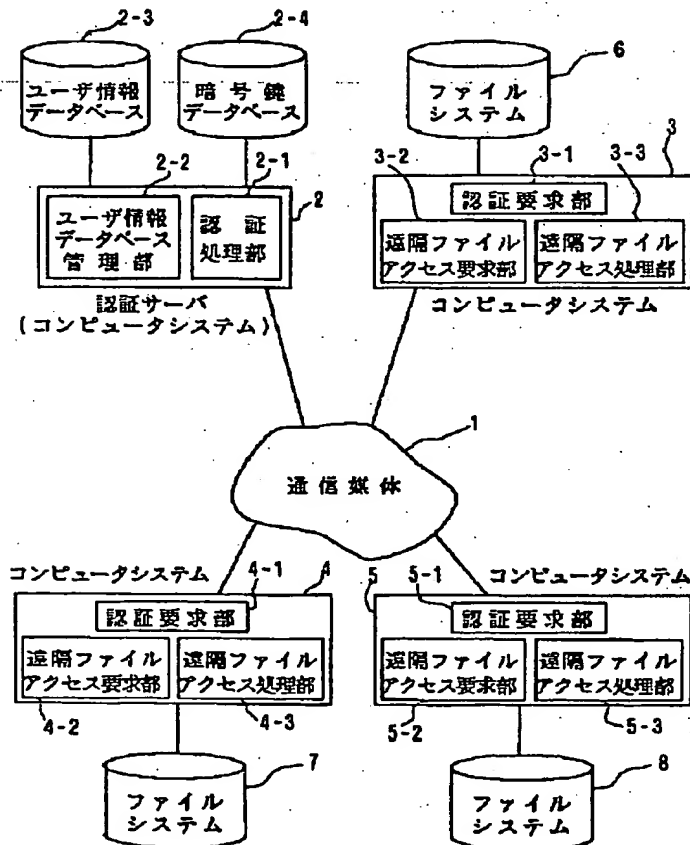
3-1~5-1 認証要求部

3-2~5-2 遠隔ファイルアクセス要求部

3-3~5-3 遠隔ファイルアクセス処理部

10 6~8 ファイルシステム

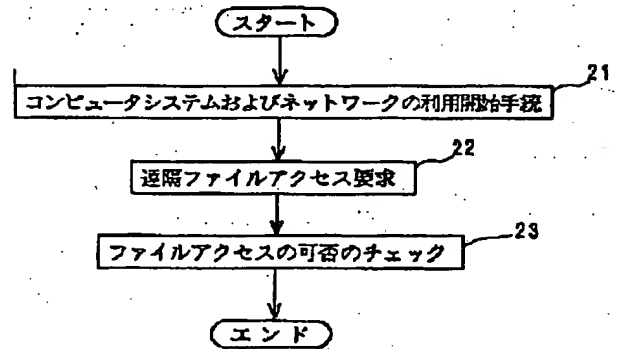
【図 1】



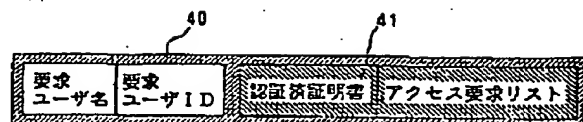
【図 3】

ユーザ名	ユーザID	認証サーバの ホスト名	認証サーバの アドレス	発行時刻	有効期限
------	-------	----------------	----------------	------	------	-------

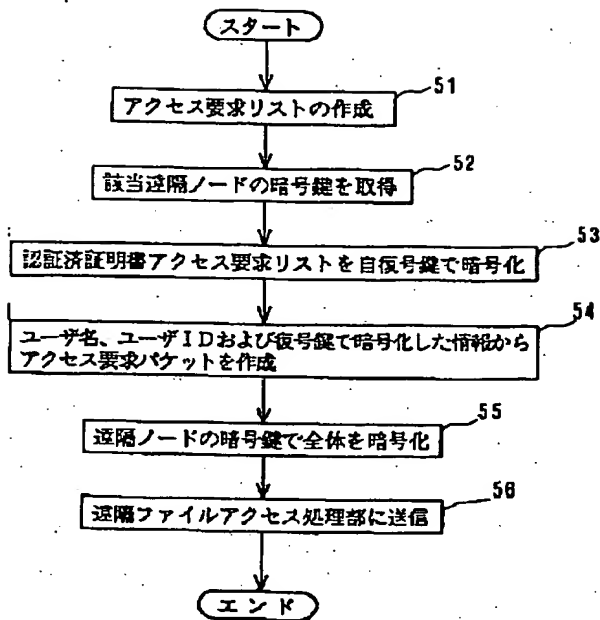
【図 2】



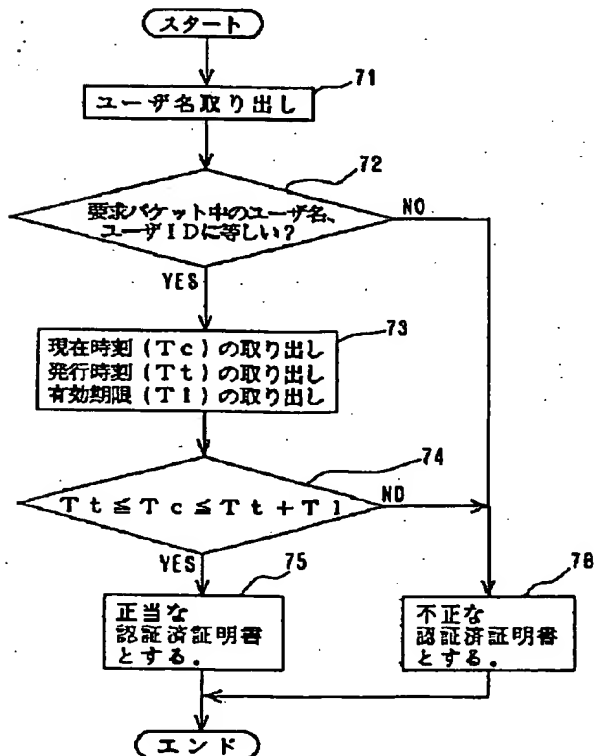
【図 4】



【図 5】



【図 7】



【図 6】

